c. receiving a response from the user based upon said challenge;
d. processing said response to verify the user;
e. assembling credentials for the transaction, said credentials comprising at least one key;
f. providing at least a portion of said credentials to said user;
g. receiving a second request from said user, said second request including said portion of said credentials; and
h. validating said portion of said credentials with said key to provide access to a transaction service.

44. (New) The method of Claim 43, wherein the transaction is an electronic purchase transaction.

45. (New) The method of Claim 44, wherein the electronic purchase transaction is conducted using a digital wallet.

46. (New) The method of Claim 43, wherein the instrument is a smartcard.

47. (New) A computer-implemented method for protecting a network server from being used as the basis of an attack on a network client, the method comprising:
a. receiving a request for a connection at said server from said network client; and
b. scanning a portion of said network server for particular characters associated with a protocol;
c. verifying that any response from said network server to said network client is void of said particular characters; and
d. providing said response from said network server to said network client.

48. (New) The method of Claim 47 further comprising restricting access to said network server for said protocol to said portion of said network server.

49. (New) The method of Claim 47 further comprising replacing said particular characters with benign characters such that a security risk posed by said selected protocol is reduced.

50. (New) The method of Claim 47 wherein said protocol comprises javascript.

A1

51. (New) The method of Claim 47 further comprising logging said particular characters to form a security log.

52. (New) The method of Claim 51 further comprising reviewing said security log to determine whether said particular characters are hostile.

53. (New) The method of Claim 47 wherein said protection of the network server is accomplished during an electronic purchase transaction.

54. (New) The method of Claim 53 wherein the electronic purchase transaction is conducted using a digital wallet.

55. (New) A transaction system for facilitating a financial transaction requested by a user operating a user computer on a data network, the system comprising:

a. a transaction authorizer; and

b. a security server configured to verify that an intelligent token is in the user's possession and to provide a digitial credential to said user computer if said verification is successful;

wherein said transaction authorizer is configured to authorize a transaction requested by said user based at least in part upon said

digital credential provided by said user computer via said data network.

56. (New) The transaction system of Claim 55, further comprising a transaction tool server.

57. (New) The transaction system of Claim 55 further comprising a wallet server in communication with said user computer via said digital network.

A1

58. (New) The transaction system of Claim 57 wherein said wallet server is configured to receive a request for a transaction from said user computer, to contact a merchant computer system, and to provide information about said user to said merchant computer system.

59. (New) The transaction system of Claim 55, wherein the user computer comprises a transaction tool and a reader, wherein said reader is configured to transfer information between the transaction tool and the intelligent token.

60. (New) The transaction system of Claim 59, wherein said transaction tool is a wallet client.

61. (New) The transaction system of Claim 55, wherein the intelligent token is a smartcard.

62. (New) The transaction system of Claim 55, wherein the connection between said security server and said transaction authorizer computer is through a data connection separate from said data network.

63. (New) The transaction system of Claim 59, wherein said transaction tool communicates with said security server via a data connection separate from said data network.

64. (New) The transaction system of Claim 55, wherein the intelligent token comprises a digital certificate that uniquely identifies the user associated with the intelligent token.

A1

65. (New) The transaction system of Claim 64, wherein the user of said intelligent token unlocks access to the digital certificate by use of a personal identifier.

66. (New) The transaction system of Claim 55, wherein the intelligent token is issued by an issuer and wherein a transaction made using said transaction system is considered a "card present" transaction as deemed by the issuer of the intelligent token.

67. (New) A digital wallet client for facilitating electronic transactions via a digital network in conjunction with a browser program, the digital wallet client comprising:

a. a wallet application configured to initiate a session with a wallet server via said digital network in response to inputs from a user; and

b. an interface to a reader device, wherein said reader device is configured to accept a token to verify the identity of said user; and wherein said wallet application is operable to authenticate said user to said wallet server using said token and to contact said wallet server via said digital network to consummate said electronic transactions.

68. (New) The digital wallet of claim 67 further comprising an activator for accessing said wallet server, wherein said activator exchanges information with said wallet server to complete said electronic transactions.

69. (New) The digital wallet client of claim 67 wherein said wallet application is further configured to authenticate said user to said wallet server based at least in part upon a credential received at said digital wallet client from a security server on said digital network.

A1

70. (New) The digital wallet client of claim 68 wherein said activator comprises a status indicator displayed to said user, said status indicator corresponding to the availability of wallet services for a web page.

71. (New) The digital wallet client of claim 69 wherein said wallet application is further configured to obtain a digital signature from said token and to provide said digital signature to said wallet server via said digital network.

72. (New) A wallet server for facilitating a transaction via a digital network, the wallet server comprising:

a. an interface to a digital network; and

b. a wallet server application in communication with a database; wherein said wallet server is configured to receive a request for a transaction from a wallet client, to process a credential received from said wallet client to authenticate a user of said wallet client, to retrieve user information from said database after authenticating said user, and to complete said transaction on behalf of said user using said user information.

73. (New) The wallet server of claim 72 wherein said credential comprises a digital signature.

74. (New) The wallet server of claim 73 wherein said credential comprises a random digest digitally signed by a token in the possession of said user.

75. (New) The wallet server of claim 74 wherein said digest is provided to said wallet client by a security server.

A1

76. (New) The wallet server of claim 72 wherein completing said transaction on behalf of said user comprises completing a merchant form with said user information.

77. (New) A computer-implemented method for facilitating an online purchase comprising the steps of:
authenticating with a security server;
receiving a credential from said security server;
identifying a merchant address from which to make said purchase;
providing said credential to a wallet server to authenticate said user to said wallet server;
upon successful authentication with said wallet server, re-directing communications with said merchant address to said wallet server such that said wallet server provides purchase information about said user to said merchant address; and
receiving a confirmation of the results of said purchase.

78. (New) The method of claim 77 wherein said credential comprises a digital signature.

79. (New) The method of claim 78 wherein said credential comprises data received from a security server.

80. (New) A computer-implemented method for facilitating an online purchase comprising the steps of:
receiving a request for a transaction from a user at a server, said request comprising a merchant address and a credential;
verifying said credential to authenticate said user;
retrieving user information from a database in response to said verifying step;
completing an online form corresponding to said merchant address; and
providing a purchase result to said user.

A1

81. (New) The method of claim 80 wherein said credential comprises a digital signature.

82. (New) The method of claim 81 wherein said credential comprises data received from a security server.

83. (New) The method of claim 82 wherein said security server is affiliated with said server.

84. (New) The method of any of claim 81 wherein said digital signature is produced by a smartcard.

85. (New) A computer-implemented method for facilitating access to a service, the method comprising the steps of:
receiving a logon request from a user;
verifying that said user is in possession of a token;
providing a credential to said user if said verification is successful;
receiving a transaction request from a user, said transaction request comprising at least a part of said credential; and
processing said at least a part of said credential to provide access to said service.

86. (New) The method of claim 85 wherein said verification step comprises a challenge-response.

87. (New) The method of claim 86 wherein said challenge-response comprises random data provided to said token.

A1

88. (New) The method of claim 87 wherein said challenge-response further comprises a digital signature of said random data.

89. (New) The method of any of claim 85 wherein said service is a financial transaction.